Comprehensive Internet Use Management
To Address the Safe and Ethical Use of the Internet in Schools

Nancy Willard, M.S., J.D.
Center for Safe and Responsible Use of the Internet
Web sites: http://csriu.org and http://cyberbully.org
E-mail: nwillard@csriu.org

Online Risky or Irresponsible Activities

The following is a comprehensive listing of the many and varied concerns about risky or irresponsible Internet use by young people. Some of these concerns directly impact schools. Others may not be directly related to school-based Internet use, but may impact the school climate or the well-being of students.

<u>Risky sexual activities</u>

- Premature exposure to pornography and other sexual materials.
  - Exposure by younger children to sexually explicit materials.
  - Seemingly endless exposure to SPAM advertising Viagra and “enhancement” patches.
- Excessive, addictive access to pornography and violent/child pornography.
  - Going beyond normal sexual curiosity to excessive, addictive access.
- Adult sexual predators.
  - Youth groomed by adult predators.
  - Youth going to online places, chat rooms, where it is clear they will meet adults interested in sex.
  - Youth posting sexually suggestive material that attracts interest of adults seeking teens for sex.
- Webcam teens.
  - Teens who are providing sexually explicit pictures and videos in exchange for gifts or money.
  - Teens may be groomed into this activity by adults or attracted by other teens.
- Hook-ups with other teens as equals or with teen predators.
  - Using Internet communities as match-making vehicle to make connections with other teens interested in non-commitment sex.
  - Posting sexually suggestive material to attract other teens interested in sex.
  - Sending sexually explicit images privately to others in context of relationship building.

<u>Cyberbullying</u>

Cyberbullying is being cruel to others by sending or posting harmful material or engaging in other forms of social cruelty using the Internet or other digital technologies.

- Flaming. Online “fights” using electronic messages with angry and vulgar language.
- Harassment. Repeatedly sending offensive, rude, and insulting messages.
- Denigration. Sending or posting cruel gossip or rumors about a person to damage his or her reputation or friendships.
- Impersonation. Breaking into someone’s account, posing as that person and sending messages to make the person look bad, get that person in trouble or danger, or damage that person’s reputation or friendships.
- Outing and Trickery. Sharing someone’s secrets or embarrassing information or images online. Tricking someone into revealing secrets or embarrassing information, which is then shared online.
- Exclusion. Intentionally excluding someone from an online group, like a “buddy list.”
- Cyberstalking. Repeatedly sending messages that include threats of harm or are highly intimidating. Engaging in other online activities that make a person afraid for her or her safety.

Cyberthreats

Cyberthreats are either direct threats or distressing material that raises concerns or provides clues that the person is emotionally upset and may be considering harming someone, harming him or herself, or committing suicide.

Unsafe Online Communities

“At risk” youth are attracted to unsafe online communities that provide information and support for unsafe, unhealthy activities. Contagion is major concern. Three basic types:

- Hate supremacy and gangs.
- Suicide and self-harm, including cutting, anorexia.
- Risky behavior, passing out, bomb-making, drugs.

Gaming and gambling

- Violent, sexual violence, hate-based violent games.
- Gaming promoted as gambling. The longer you play the greater the potential of financial return.
- So-called “risk-free gambling” games on teen community sites.
- Underage gambling on online gambling sites.
- Advergaming. Integrating commercial messages into children’s online games

Hacking and hacker tribes

- Engaging in activities to gain access to secure sites.
- Engaging in group efforts to commit criminal computer security violations.

Copyright infringement

Downloading or disseminating copyrighted material, generally entertainment or software.

Plagiarism

Incorporating material written by others into student work product, without proper quotation or citation.

Security concerns

- Engaging in activities that can increase security risks from viruses, worms, Trojans.
- Providing personal information in ways that can result in identity theft.
- Scams. Being defrauded in some way

Foundational Concerns

Underlying the above listed behaviors are issues of concern that are more foundational and impact many of the above behaviors.

Privacy

Young people appear to have limited to no concept that what they post on the Internet in online communities to totally public and permanent or that what they share through private communication can be preserved and made public and what the possible short-term or long-term consequences of such disclosure might be. Need to distinguish between:

- Personal contact information, Should only be shared on a secure site when necessary to accomplish specific purpose.
- Intimate personal information, Should never be shared in public communications, possibly can share with totally trustworthy friends through private communications, understanding risks, may be shared on professional support services sites.
- Personal interest information. Generally safe to share.

Internet addiction

Excessive amount of time spent using the Internet, resulting in lack of healthy engagement in other areas of life. Is itself a concern, as well as an indicator of other concerns.

Information literacy

The ability to know when there is a need for information, to be able to identify, locate, evaluate, and effectively use that information for the issue or problem at hand.

Stranger literacy

The ability to determine the relative safety and veracity of individuals with whom one is communicating online who are unknown in person

Eyeballs and e-wallets

Understanding the degree to which so-called “free” commercial online services are supported by marker research activities (profiling) and advertising, including imbedded marketing and viral marketing and “stickiness,” which is how commercial sites encourage long and frequent access to their site.

Multi-tasking

Recognizing the perils of multi-tasking and gaining the ability to prioritize and focus on important tasks.

Influences on Online Behavior

How the use of online technologies can impact safe and responsible decision-making.

You can’t see me

When people use the Internet, they perceive they are invisible. The perception can be enhanced because they create anonymous accounts. People are not really invisible, because online activities can be traced. But if you think you are invisible, this removes concerns of detection, disapproval, or punishment.

I can’t see you

When people use the Internet they do not receive tangible feedback about the consequences of their actions, including actions that have hurt someone. Lack of feedback interferes with empathy and leads to the misperception that no harm has resulted.

Everybody does it

The perception of invisibility and lack of tangible feedback support risky or irresponsible online social norms, including:

- “Life online is just a game.” Allows teens to ignore the harmful “real world” consequences of online actions and creates the expectation that others will simply blow off any online harm.
- “Look at me—I’m a star.” Supports excessive disclosure of intimate information and personal attacks on others, which is generally done for the purpose of attracting attention.
- “It’s not me. It’s my online persona.” Allows teens to deny responsibility for actions taken by one of their online personas or identities.
- “What happens online, stays online.” Supports the idea that one should not bring issues related to what has happened online into the “real world” and should not disclose online activity to adults.
- “On the Internet, I have the free speech right to write or post anything I want regardless of the harm it might cause to another.” Supports harmful speech and cruel behavior as a free speech right.
- “If I can download it, it must be free.” Supports the idea that material that can be freely disseminated through the Internet, generally entertainment media or software, there ought to be no charge for it.
- “If I can do it, it must be okay.” Supports the idea that if something is technically possible it ought to be considered acceptable.

Youth At Risk

Which youth are more “at risk” online? Obvious answer: Youth who are already “at risk” are more at risk of being victimized online.

Why?

- They are “looking for love in all the wrong places”
- They post clues to their distress, which is advertising for predators and other “at risk” youth.

- Predators find them and start to groom them.
- They form online communities with other “at risk” youth.
- Involvement within these groups leads to contagion
- Involvement with predator or group leads to strong belief that, at long last, they have found true friendship and acceptance

Who?
Youth who are depressed, angry, have suicidal thoughts, are considered “losers” at school, have no friends, have difficult relationships with parents, are withdrawn, are questioning their sexual orientation, or are sexually interested or provocative.

What Is Not Working
What is not working is simplistic rules and overreliance on filtering.

Simplistic Rules

Many times Internet safety education is delivered to youth in the form of simplistic rules, generally presented by an adult assuming an “authoritarian” role.

Examples
- Do not provide personal information online.
- If you see something online that upsets you, tell an adult.
- Remember that people online might not be who they say there are.

Problems
- Adult delivered. Teens are unlikely to listen to adults, who they suspect know far less than they do about the Internet, especially when the adult assumes the role of an authority figure.
- Not age-based. Concerns for 8 year olds are different than concerns for 14 year olds.
- Not activity-specific. Providing personal contact information on a secure site to purchase online is not same as providing personal contact information in a social networking community.
- Not sufficiently detailed. Information on risks or concerns that rule seeks to address is generally absent. It is necessary to understand the risks to effectively make safe and responsible choices. Information on how to accomplish desired online activities without undue risk is generally absent.
- Not comprehensive. Rules do not directly address major concerns.

Better Approach
- Younger children need to use the Internet only in safe places established by adults, with very simple rules:
    - Do not type your full name on the computer or provide any other information about who you are or where you live. Teach how to use username even for computer games.
    - If anything “yucky” comes up on the screen, turn off the screen like this and tell your parent or teacher.
    - Do not access sites outside of the protected area without permission and assistance from your parent or teacher.
- Teens need knowledge, skills, and motivation sufficient to enable them to make safe and responsible choices.
- And adult supervision of all public online activities and review of private communications, if there is a reasonable suspicion they are not making safe and responsible choices.

Filtering Follies

- 65% of US homes where children/teens use the Internet relying on filtering software.
- CIPA requires all schools and libraries to install filtering
- And in a few months the US Department of Justice will be going to court to prove that filtering does not work.

What is going on?

- Since at least the time of the invention of the printing press, dissemination of pornography has been an engine for technological advancement and adoption
- Early Internet, pornography was primarily disseminated through newsgroups. Because Universities were the only ones connected to the Internet, they became major purveyors of porn
- As the Internet became commercialized all new technologies have immediately become mechanism for dissemination of porn – web, P2P, streaming video, …
- 1995. Time magazine raised public attention to concern of online porn. The news report was based on bogus research, but concerns were real.
- 1996. Congress enacted Computer Decency Act. CDA prohibited distribution of obscene material to minors through the Internet.
- 1997. The Supreme Court upheld a lower court ruling that CDA was unconstitutional.
- 1997. Internet Online Summit Focus on Children was held – hosted by Vice President Al Gore, including representatives of Internet industry, various advocacy groups from across the spectrum, schools, and libraries. Resulted in strong promotion of "user empowerment tools" to help parents and others shield children from inappropriate material.
- 1999. Congress enacted Children's Online Protection Act. COPA required commercial distributors of material harmful to minors to protect their sites from access by minors. ACLU immediately challenged COPA arguing that filtering is a less restrictive alternative.
- 2000. Congress enacted Children's Internet Protection Act arguing that if filtering is the solution, the places where youth are accessing the Internet, schools and libraries, should use filtering. Strongly promoted by conservative religious organizations and opposed by civil liberty groups. ACLU and ALA challenged CIPA. But ACLU was in a bind because of its argument in COPA. Evidence was presented on concerns of overblocking, but no evidence presented on concerns of underblocking.
- 2003. Supreme Court held CIPA constitutional because filtering is an effective solution and filters can be easily overridden to provide access to inappropriately blocked material – but specifically noted that if filtering was implemented in a way that it could not easily be overridden to provide access, this could raise constitutional concerns – a point that the vast majority of school districts are ignoring.
- 2003. US government's Voice of America program provided funding to Peacefire, a filtering proponent, to develop a free software program that can easily be installed on PCs to circumvent any filtering – resulting in creation of Circumventor
- 2004. Supreme Court issued a ruling on COPA. The Court ruled that the law was probably unconstitutional because filtering is a superior and less restrictive alternative, but sent case back to trial level since there had been so many changes in laws and technologies since the first trial.
- 2006. A new COPA trial will be held. To prevail, DOJ must prove that filtering does not work. The ACLU must prove that filtering does work. Clearly, DOJ will establish that filtering does not work.

In sum

US Government

- Enacted COPA requiring age verification – but COPA clearly will not prevent dissemination of porn because Internet is international and porn purveyors will simply move their operations off-shore. Federal ban on online gambling does not work either.
  Enacted CIPA requiring schools and libraries to spend billions of dollars to install filtering
- DOJ defended CIPA, arguing that filtering works and is necessary.
- DOJ is now defending COPA, arguing that filtering does not work.
- Voice of America funded development of software that makes it easy to circumvent any filter.

ACLU and other civil liberties groups

- Challenged CIPA, arguing that filtering does not work because filters overblock.
- Challenging COPA, arguing that filtering works and is a less restrictive alternative.

Internet industry

- Promote filtering as a reasonably effective solution because wants parents to allow children to spend lots of unsupervised time on the Internet.

- Advertises “safe online environments” to parents at same time is promoting massive advertising for kid-related products to children within these environments.
- Some companies are concerned about off-shore migration of porn purveyors due to anticipated loss of revenue.
- Filtering companies probably concerned that DOJ’s case will damage their market.

Conservative Organizations and Filtering Companies

- Conservative organizations strongly promote filtering.
- Some filtering companies appear to be “in bed” with conservative organizations, including companies whose products are used in public schools
- Many filtering products block “liberal-perspective” sites that provide information on gender orientation, safe sex, abortion/morning-after, and non-traditional religions, but do not block “conservative-perspective” sites on same subjects. Use of products that block in this manner is clearly unconstitutional.

Parents

- Significant overreliance on filtering.
- Are not supervising children’s Internet use effectively, probably because of false security due to reliance on filtering.

Schools

Significant concerns about current practices in Internet use management, especially in the contect of social networking.

<u>The truth about filters</u>

- Filters can provide some protection against access to sites deemed unacceptable.
- Filters have significant failure rate in blocking access to harmful materials.
- Filters frequently overblock and prevent access to appropriate materials, sometimes inadvertently and sometimes apparently based on inappropriate, conservative bias.
- Filtering companies frequently establish categories where they block access to sites containing material that should be appropriate for youth along with material that would not be considered appropriate.
- Filters can easily be circumvented by using proxies or innovative access techniques.
- Reliance on filtering has led to perception that filtering can address all Internet use concerns and a failure to focus on human factors, especially standards for use and effective monitoring and supervision.

Concerns about Managing Internet Use in Schools

<u>Internet “recess”</u>

- Excessive use of district Internet system for entertainment or other non-educational activities.
    - Are students using the Internet for education or playing around?
- Inadequate approach to integration of technology for instruction.
    - Are technology-related instructional issues managed by computer services or curriculum and instruction department?
- Inadequate curriculum development and professional development.
    - Do you have a separate section of instructional objectives related to computers or has thought been given into how technologies can enhance learning in key academic areas?
- Failure to require educational purpose for Internet use, which should include quality non-class-related research, but not social networking or games.
    - What are your policies and practices related to use of computers?
- Lack of accountability.
    - Are you tracking the manner in which computers and the Internet are actually being used and are impacting student learning?

Constitutional concerns
Rights of Students to Access Information
Board of Education, Island Trees Union Free School District No. 26 v Pico standard:

> (T)he state may not, consistent with the spirit of the First Amendment, contract the spectrum of available knowledge. In keeping with this principle, we have held that is a variety of contexts the Constitution protects the right to receive information and ideas....
>
> In our system, students may not be regarded as closed-circuit recipients of only that which the State chooses to communicate. ...[School] officials cannot suppress 'expressions of feeling with which they do not wish to contend.
>
> (J)ust as access to ideas makes it possible for citizens generally to exercise their rights of free speech and press in a meaningful manner, such access prepares students for active participation in the pluralistic, often contentious society in which they will soon be adult members. ...
>
> (S)tudents must always be free to inquire, to study and to evaluate, to gain new maturity and understanding. The school library (and Internet system) is the principle locus of such freedom. ... In the school library (and through the Internet), a student can literally explore the unknown, and discover areas of interest and thought not covered by the prescribed curriculum.

- With commercial filtering products, there is no access to information about how filtering decisions are made by the company and no public accountability. Some companies are clearly blocking access based on conservative bias.
  - Do you know the blocking standards of the company whose product your district is using? Are these standards in accord with students' constitutional rights of access to information?
- At the school level, decisions on categories and sites to block are frequently not made by people who understand students' constitutional rights.
  - Who has made the decisions about what categories and sites to block and on what basis were these decisions made? Were decisions to block categories or sites made on "CYA" basis?
- The reason the Supreme Court upheld CIPA was that filters could easily be overridden to provide access to inappropriately blocked sites and the court indicated that if such access were not provided, this could raise constitutional concerns.
  - Have you established an effective and timely process to quickly override inappropriately blocked sites?

Emerging Concerns
Youth involvement in social networking communities is creating new challenges for schools.

- Totally off-campus activities are interfering with the school social climate and well being of students.
  - Students are trying to get to these sites through the district Internet system, including circumventing the filter to do so.
  - Students are using mobile communication devices while in school to engage in social networking
- Internet addiction
  - Youth have become excessively engrossed in these online social networking communities, which can lead to school failure.
- Cyberbullying
  - Youth are engaging in cruel online behavior that is harming the well being of students, the school social climate, and is leading to incidents of school violence and youth suicide.

Social Networking Opportunities and Risks

Opportunities
The new social networking tools, blogging and wikis, are incredibly important tools for collaborative learning and creation. Use of these tools provides:

- Necessary skills for success in further education and workplace.

- The opportunity to impart important lessons about safe and responsible choices in these environments.
- New exciting ways to engage students.

Risks

Use of these tools raises other concerns related to publication of youth-created material. The major concerns include:

- Harmful speech.
  - Defamation.
  - Disclosure of personal contact information or intimate information about self or others.
- Intellectual property concerns.
  - Plagiarism failure to cite or quote properly.
  - Copyright infringement.
- Academic freedom concerns.
  - Online presence a wide range of student viewpoints could lead to community controversy.

Comprehensive Internet Use Management in Schools

Comprehensive planning and implementation

Who needs to be involved?

- Curriculum and Instruction.
- Library Media.
- Computer Services.
- Should establish an interface with school safety committee.

Needs Assessment

Regular assessment and analysis is the foundation for accountability. Need to know:

- How are teachers and students using district technology resources?
- How well prepared are teachers to effectively use district technology resources? Teacher perceptions and student perceptions.
- How frequently are students or teachers being blocked from accessing sites that they think might contain relevant information?
- How rapidly is the filter overridden to provide access and how effectively is this working?
- What filter is used, what categories are blocked, what is reason for blocking categories, what is the potential for biased blocking?
- Are online resources that could be helpful for instructional activities being blocked? (eg. Google images)
- Are there instructional activities that teachers would like to engage in that are currently restricted, if so what and why?
- Are students being cyberbullied by other students under conditions where this may be occurring through district Internet system or through mobile communications used during school?
- Are students being cyberbullied by other students outside of school?

Essential Components of Comprehensive Approach

Age-based Approach

- Elementary students do not have developmental capacity to be trusted to make safe and responsible choices on wide-open Internet.
  - Use should be in “safer online places” previewed sites and closely controlled communications.
- Middle and high school students should have the knowledge, skills, and motivation to make good choices.
  - Should be allowed wider access, but under conditions of effective supervision and monitoring.
- Teens need access to sensitive health information, including sexual health information – which is likely to create the most controversy.
  - Develop district web page that provides access to sensitive health information and education sites that meet established standards for accuracy and appropriateness for a teen audience.

Educational Purpose

“Where you tend a rose, a thistle can’t grow.” (Secret Garden)

The district Internet system should be used for educational activities, which should include high quality self-interest research, but not entertainment activities.

- When students use computers, such use should be for a clearly defined educational activity.
- Determine how to manage any “open access” use, such as use in the library.
- Effective curriculum and professional development is the foundation for promoting effective educational use.

Clear, Well-communicated Policy

- Internet use policy provisions should be revisited in light of needs assessment findings and new/emerging concerns.
- Policy should be integrated with disciplinary code and should be enforced.
- No need for student/parent signature for simple Internet use. But signature advisable for any postings of any student work or pictures online. Determine standards for each school level (elementary, middle, and high) and include permission statement in enrollment documents.
- Policy should address:
    - Educational purpose requirement
    - Prohibited online activities
    - Privacy and communication safety requirements
    - Establishment of limited expectation of privacy in records of online use
    - Provide reminders of provisions during log-on and through posters in labs
    - Provide online report feature to confidentially report any Internet use concerns.

Education of Students about Safe and Responsible Use of the Internet

Internet use policy provides foundation for this instruction. Unfortunately no comprehensive Internet safety education curriculum available

- Elementary students:
    - Simple rules as discussed above.
    - Specifically address risky online sexual activities in conjunction with sex education in fifth grade, using NetSmartz curriculum from NCMEC.
- Middle and high school students:
    - Specific instruction about provisions of Internet use policy at first of every year
    - Integrate Internet safety and responsible use discussions into appropriate classes:
        - Copyright and plagiarism into library, language arts classes.
        - Risky online sexual behavior into health classes.
        - Cyberbullying into classes that address social skills.
        - Safe and responsible online publishing in any class where students are posting information online.

Supervision and Monitoring

- Students have limited expectation of privacy when using the Internet in schools, similar to “locker search” standard.
    - All use of computers in school is considered in “plain view,” subject to review at any time by a staff person.
    - General supervision and monitoring is to be expected at all times.
    - Individualized search of Internet use records will occur when reasonable expectation that student has violated district rules or evidence of other safety concerns.
    - Establish standards on how, when, and by whom an individualized search should be conducted.
- Supervision is provided by teachers.
    - Computers should be placed for effective viewing.
    - Require students to print history file after time in computer lab.
- Monitoring is done with technologies.

Technology Protection Measures

Technical Monitoring

- Consider use of real time electronic monitoring or intelligent content analysis monitoring system that tracks all Internet use and provides reports of online activity that has indicators that raise concerns of misuse.
- Notice of monitoring is an important deterrent.

Filtering

- Continue to use filtering software to block access to pornography to meet requirements of CIPA.
- Consider shifting to open source system that provides complete information about blocked sites.
- If continue to use commercial filtering software
- Carefully review categories limiting selection to essential categories that are not blocking based on bias.
- Implement effective system to override inappropriately blocked sites.
- Ensure that filter does not block selected student health information sites.

Address the Social Networking Risks

Policies

- Policy provisions should be reviewed to ensure they are adequate to protect against social networking risks.
- All student material should be reviewed by teacher prior to placement on any district web site.
    - All technology tools for such placement must be under teacher control.
        - District implemented technologies
        - District approved external services
- Teachers need specific professional development about risks associated with online publishing.
- Standards should be established for teachers.
    - Inform supervisor of intention to publish student material online or engage students in social networking instructional activities
    - Provide lesson plans
    - Planned activities and instructional objectives
    - How activities will be technically managed
    - Standards teacher has established to manage risks
    - How students will be instructed about safe and responsible online publishing
    - Process of informing parents

Establish a "Web Site Concerns" link

On the district site, school web sites, and any site with student work or social networking activities have a link that reads: "web site concerns."

"XYZ District seeks to ensure that all materials placed on the district or school web sites are placed in accord with copyright law and do not infringe on the rights of others or harm others in any way. To accomplish this we are taking three steps:
- We have provisions in our Internet Use Policy that address copyright, plagiarism, defamation, invasion of privacy, and other harmful speech.
- We have established web site management procedures to review materials prior to their placement on the web site.
- We will promptly respond to any issues of concern. If you have a concern about material placed on our web site, please contact us. <link to e-mail to an administrator who has the responsibility of promptly responding to any complaint>"

Address free speech standards and academic freedom

Balancing control with academic freedom

- Hazelwood standard. School web site would be considered school-sponsored communication, so the district may place reasonable educational restrictions on student speech.
- However, district should support academic freedom, rights of teachers to explore controversial subjects, and the rights of students to express opinions on controversial issues.